



VMware vCenter Configuration Manager Security Environment Requirements

VMware VCM 5.4.x

WHITE PAPER

Table of Contents

1.0 Introduction to The Security Environment of VCM.....	5
2.0 Background Concepts.....	6
3.0 Secure Domain Infrastructure.....	9
3.1 Domain controller is trusted.....	9
3.2 Network infrastructure is secure.....	9
3.3 Network infrastructure services are available.....	9
3.4 'Trusted' certificates, certificate authorities, and certificate servers are trusted.....	9
3.5 Network infrastructure hosts are at least as secure as VCM.....	10
4.0 Hosting Environment.....	11
4.1 VCM servers are secured and managed like network infrastructure.....	11
4.2 UI Zone machines should be subject to access controls.....	12
4.3 Data originating from a managed machine is no more trustworthy than the machine.....	12
4.4 Server zone machine dedicated to VCM.....	12
5.0 Personnel Selection and Training.....	13
5.1 VCM accounts are granted to users who are trusted, trained, and qualified as system and network administrators.....	13
5.2 VCM users are advised to treat direct login prompts to VCM with skepticism and caution.....	13
5.3 VCM users must protect collected data as confidential information.....	13
5.4 Trust individual collection results no more than their source.....	13
5.5 Beware of cross-site scripting attacks.....	14
5.6 Exported data is outside the control of VCM.....	14
6.0 Host Preparation and Management.....	15
6.1 VCM hosts pass Foundation Checker checks.....	15
6.2 Cryptographic service providers are FIPS-140 certified.....	15
6.3 SQL Server best practices are followed.....	16
6.4 Only trusted software should be installed in the server zone.....	16
6.5 Perform routine backups, patches, and virus scanning.....	16
7.0 Safeguarding Installation Kits.....	17

7.1 VCM installation kits are obtained from VMware or secure sources.....	17
7.2 VCM installation kits are protected from tampering or verified.....	17
7.3 Unknown software publisher warnings during ClickOnce installations are not dismissed unless.... the publisher is VMware.....	18
7.4 Automatic upgrade of the VCM Remote Client is not used to install software.....	18
8.0 IIS Preparation.....	19
8.1 IIS set to use Windows integrated authentication for the VCM Web site root.....	19
8.2 VCM Web Service uses HTTPS.....	19
8.3 SSL/HTTPS certificate issued by trusted CA or self issued.....	19
9.0 SQL Server Preparation.....	20
9.1 Follow Microsoft SQL Server configuration best practices.....	20
9.2 Protect SQL Server from connections originating outside the server zone.....	20
9.3 Forbid direct SQL Server login by VCM users.....	20
10.0 Web Browser Preparation.....	21
10.1 Place the VCM Web host in the IE trusted zone.....	21
10.2 Verify the VCM Web host's HTTPS certificate.....	21
10.3 Verify the VCM software publisher certificate.....	21
10.4 Remove untrusted machines from the IE trusted zone.....	21
10.5 Customize Internet Explorer's trusted zone Internet security options.....	22
11.0 Agent Installation and Maintenance.....	23
11.1 File and directory access controls prevent tampering.....	23
11.2 Access control on machine configuration prevents tampering.....	23
11.3 The Agent is available for collection.....	23
11.4 The Trusted Certificate Store contains reputable certificates.....	24
11.5 The enterprise certificate authorized collection.....	24
11.6 Unauthorized (private) Agents are not allowed.....	24
11.7 Continuous possession and control of the Agent.....	24
12.0 Software Provisioning Components.....	25
12.1 All published packages are signed by trusted parties.....	26
12.2 Protect repositories.....	26
12.3 Accept only reputable software package publishers.....	26

12.4 Configure only trusted sources over secure channels.....	26
12.5 Take precautions when using VCM Software Provisioning Extensions.....	26
13.0 Operating System Provisioning Components.....	28
13.1 Provisioning zone is secure.....	29
13.2 Dedicated OS provisioning server host.....	29
13.3 Close unnecessary ports on the OS provisioning server.....	29
13.4 Protect baseline OS images.....	29
13.5 Preserve SSL tunnel.....	29
13.6 Protect credentials.....	29
14.0 Proper Decommissioning.....	31
14.1 An installation of VCM is properly decommissioned before its hardware is repurposed or retired.....	31
14.2 Collector and Agent private keys used for TLS are not copied between machines.....	31
14.3 Enterprise certificate private key and IIS (for HTTPS) host private keys are transferred manually..	32
14.4 Server zone hosts have their disks removed and transferred, secured, or erased before decommissioning.....	32
14.5 Erase private keys when uninstalling the Agent.....	32
14.6 Unused network authority accounts are disabled or removed.....	32
References.....	33

1.0 Introduction to The Security Environment of VCM

VCM operates within the context of a security environment. This environment consists of host configuration, various personnel and usage assumptions, organizational security policies, configuration settings, and best practices. Ultimately all security requirements are met either by controls built into VCM that leverage the environment, or by controls built into the environment itself. Understanding and maintaining the security environment is an important responsibility of the VCM administrator and users. Toward that end, this document provides a description of the VCM security environment and a checklist for its maintenance.

The security environment must provide certain guarantees. For example, authorized VCM users are presumed to be trusted, and the hosts on which VCM is installed must be access-controlled to prevent access by unauthorized users. Installation kits must be checked for alteration, and eventually VCM hosts must be decommissioned properly. Overall security requirements must be observed for the domain and infrastructure, hosting environment, personnel, host preparation, installation kit security, login roles, IIS preparation, SQL server preparation, web browsers preparation, Agent installation and maintenance, and proper decommissioning.

When a security environment requirement is not met, the confidentiality, integrity, or availability of information assets that flow through the deficient system are at risk.

This is not a prescriptive document. Described within are the assumptions made by VCM, not procedures for administrators. For example, under the guarantees regarding VCM logins, an assumption made by VCM is that the domain controller for each user is trusted. Not listed is a best practice such as "keep the domain controller in a locked room."

2.0 Background Concepts

Numerous physical and conceptual objects make up a VCM installation. These are described in detail in the *VCM Hardware and Software Requirements Guide* as well as in the *VCM Installation and Getting Started Guide*. For convenience, a summary of that information is repeated here.

VCM is a distributed application with five main components:

- Browser-based user interface (UI) that renders in Internet Explorer (IE) on user desktops
- Internet Information Services (IIS) web server that hosts the UI web application and accepts work requests
- Collector service that processes requests and receives results
- SQL Server database that stores both results and application control information
- Agents that inspect managed machines and return results in response to requests.

In some installations there are also optional ancillary components such as an Agent proxy that works with VMware ESX, ESXi, and vSphere servers, an orchestration host that coordinates with service desk applications such as Remedy, VCM Remote service, Operating System Provisioning, Software Provisioning components, and alternate source file servers that store VCM installation kits and VCM Patching patches.

With the exception of the UI, Agent, alternate sources, and OS Provisioning Server, all VCM components execute on Microsoft Windows Server computers. The UI runs within IE on Windows desktops. The Agent executes on either Windows or one of a variety of UNIX systems (Solaris, HP-UX, AIX, Linux, or Mac OS X). An alternate source can be any file server exporting shares or ftp.

These components, with the exception of the UI Software Provisioning Repositories, and alternate source hosts, are shown below.

These components, with the exception of the VCM Software Provisioning components, the UI, alternate source host, and the OS Provisioning Server, are shown below. Software Provisioning components are diagrammed separately in [Software Provisioning Components on page 25](#).

vCenter Configuration Manager Security Environment Requirements

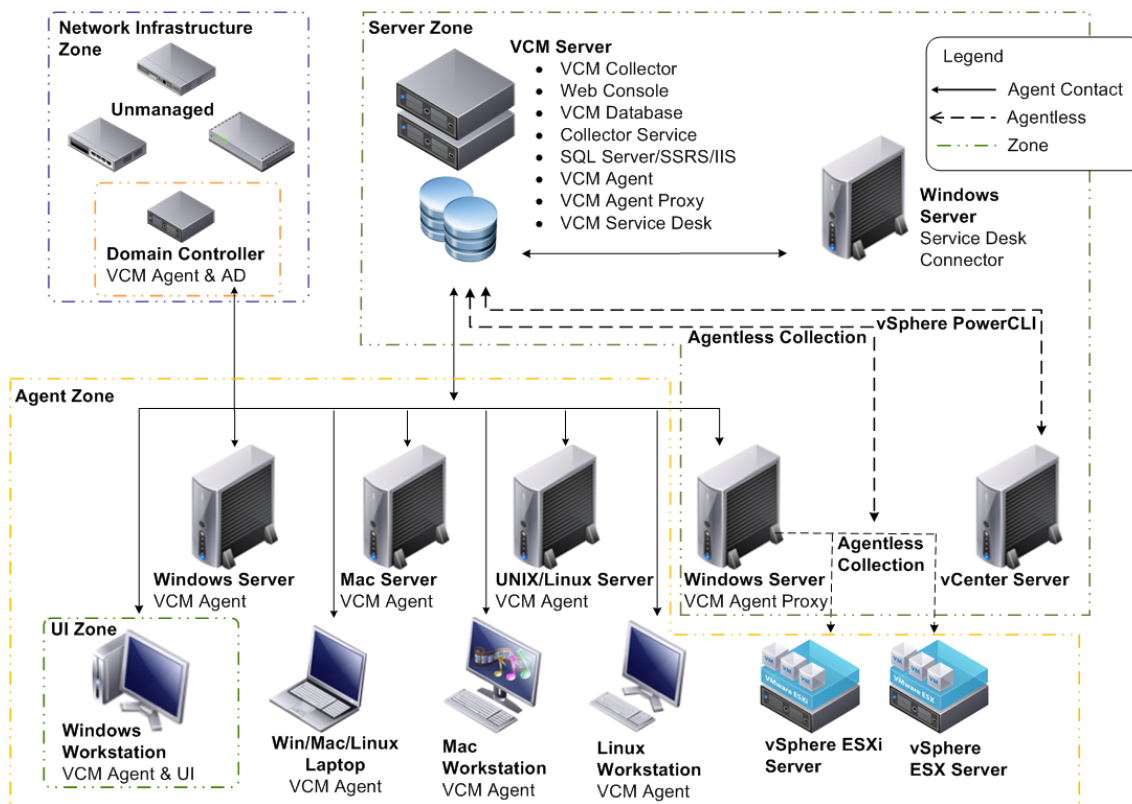


Figure 1: VCM Server Installation

IIS, the web application, SQL Server, and the Collector service are installed on a server machine referred to as the “Collector host”. Several different types of personnel utilize the five components of VCM. Domain administrators create the accounts and manage the infrastructure in which VCM runs. The infrastructure includes domain controllers, routers, certificate servers, SMTP email, domain name service (DNS) and DHCP. A VCM installer loads the VCM software and configures IIS, SQL server, the Collector, and other services. The installer is also the first VCM administrator and is responsible for authorizing the other administrators and regular VCM users from the inventory of accounts managed by the domain administrators. VCM users and administrators log on to VCM and use its web interface to administer managed machines via the Agents, run Compliance tests, and generate reports. Agents can be installed, upgraded, and un-installed by either VCM administrators, users or managed machine administrators.

Conceptually, the VCM services, hosts, and personnel can be organized into the following trust zones:

- **Infrastructure:** Consists of domain controllers (DCs), routers, SMTP, DNS, and other infrastructural items.
- **User Interface (UI):** Consists of VCM user desktops.
- **Server:** Consists of the Collector service, VCM Remote service, IIS, web application, SQL Server, Orchestrator, and Agent proxy.
- **Agent:** Each managed machine, software provisioning repository, and alternate source resides in an Agent zone. There may be multiple Agent zones.
- **Provisioning:** Consists of the OS Provisioning Servers, provisionable target hosts, and the network infrastructure that connects them.

Domain administrators manage the infrastructure, UI and server zones. Each Agent zone is controlled by a local zone administrator. This is often the managed machine or repository administrator

This partitioning allows us to understand trust between VCM components on a more granular level than DC domains. A trust boundary separates each zone. Machines and services in one zone distrust those in another without either special configuration or authentication. Special configuration establishes implicit trust. Authentication engenders trust between components lacking implicit trust. When an entire zone trusts another, this means that every VCM component in the first zone implicitly trusts every component in the second. If two machines are in the same zone, it does not mean that they trust each other, rather it means that they are not required to distrust each other by default. Once VCM is installed, the UI and Agent zones trust the infrastructure and server zone. On the other hand, the server zone completely trusts only the infrastructure; it does not trust the UI zone except as a source of UI commands from VCM users that were authenticated by the infrastructure. The server zone also trusts the Agent zone as a source for Agent data but not to provide data or implement change that would affect other Agents or VCM configuration.

These trust zones and boundaries are pedagogical tools, and are not visible in the features of the VCM product. The trust zones have no relationship to the zones in IE.

3.0 Secure Domain Infrastructure

VCM security environment requirements are divided into categories for the domain and infrastructure, hosting environment, personnel, host preparation, safeguarding installation kits, login roles, IIS preparation, SQL Server preparation, web browser preparation, Agent installation and maintenance, Software Provisioning, OS Provisioning, and proper decommissioning.

This section describes the domain and infrastructure. Here and in subsequent sections, each requirement is numbered, stated, and followed by elaborative text.

3.1 Domain controller is trusted

VCM relies on a domain controller (DC) to authenticate VCM users, to discover machines, to enumerate domain group members, to run VCM services under Network Authority accounts, and to authenticate administrators who control the hosts onto which VCM and its databases are installed. The VCM installer and VCM administrator cite the domain controller in VCM when the system is installed, DC discoveries are conducted, or when new Network Authorities or VCM users are added. An untrustworthy domain controller should never be configured into VCM and VCM hosts should never be joined to an untrustworthy domain.

3.2 Network infrastructure is secure

Besides domain controllers, VCM relies on other network infrastructure services such as DNS, WINS, email, time servers, and DHCP. The DNS and WINS translate domain names into IP addresses. Email is used for various notifications and alerts. Time servers synchronize time, allowing Kerberos authentication and certificate validation to work. DHCP, even when not used by VCM servers, assigns IP addresses consistently. These services must be properly configured, secure, and available in order for VCM to operate correctly and reliably.

3.3 Network infrastructure services are available

All network infrastructure services must not only be correct and secure, but also available and responsive. An active denial of service or attack on network infrastructure will impact VCM performance.

3.4 'Trusted' certificates, certificate authorities, and certificate servers are trusted

VCM establishes the validity of HTTPS/SSL certificates used by IIS, and of TLS certificates used during Collector-to-Agent communication by checking the signatures along the certificate chain that extends from the certificate in question up to a certificate installed in one of the trusted certificate stores.

VCM trusts that:

- A certificate in a 'trusted' store is in fact trusted
- Certificate authorities issuing certificates in a trusted store are trusted
- Certificate services managing certificates in a trusted certificate store and the associated renewals and certificate revocation lists are trusted

In particular, certificates that exist in the trusted store that were not issued in conjunction with VCM are still trusted by VCM.

To view the contents of the trusted certificate stored on Microsoft platforms¹, use the Certificate Manager Tool (Certmgr.exe) or the Microsoft Management Console (MMC) Certificates snap-in.

3.5 Network infrastructure hosts are at least as secure as VCM

Since VCM relies on infrastructure services, machines on which these services are hosted must be at least as secure as VCM. These machines should be protected by firewalls, anti-virus software, current security updates, and access controls. Access to these machines should also be restricted to trusted personnel.

4.0 Hosting Environment

This section describes the security environment that must be maintained on the hosts onto which components of VCM are installed.

4.1 VCM servers are secured and managed like network infrastructure

VCM servers are hosts in the server zone. These hosts store and manipulate collected data and change requests for every managed machine.

As such, these servers should adhere to the following requirements:

- Servers should not be open to general users.
- Servers should be protected from the open Internet by firewalls.
- Servers should be completely trusted by managed machine administrators.
- Operating systems on these servers should be updated to the most recent current patch level.
- Servers should be backed-up on a routine basis.
- Each server should be running an operating system with mandatory user logins enabled.

If infrastructure hosts like domain controllers are managed by VCM, hosts in the server zone should be treated and managed with measures consistent with those used for the infrastructure.

Each VCM server should also be running an operating system that conforms to the Common Criteria Controlled Access Protection Profile (CAPP)². The CAPP ensures that:

- Access to the host is protected by a certified authentication process
- User data is protected from other users
- Security functions of the operating system are protected from unauthorized changes

Windows 2000, 2003, XP, and Vista, 2003 Server, and 2008 Server conform to the CAPP³. Windows 7 and Windows 2008 Server R2 are in evaluation as of November 2009.⁴

4.2 UI Zone machines should be subject to access controls

The hosting environment for machines in the UI zone is less stringent than in the server zone. UI machines do not need to be protected by firewalls or isolated from the Internet. However these machines should still:

- Run operating systems that meet the CAPP
- Be patched to the latest security level
- Run anti-virus software

4.3 Data originating from a managed machine is no more trustworthy than the machine

Managed machines have no prerequisite security requirements. Instead, the security of each machine determines the degree to which data originating from that machine can be trusted. VCM users must be aware that data collected from an unsecured machine connected to the Internet is less reliable than data collected from an infrastructure host walled off in a corporate VPN.

4.4 Server zone machine dedicated to VCM

VCM relies on the server operating system to protect the confidentiality, integrity, and availability of server zone data from other services or users running on the VCM server hosts. When server zone machines are used for purposes other than VCM, then you risk granting unintended access to VCM data if those services (or users) have machine administrator rights.

5.0 Personnel Selection and Training

5.1 VCM accounts are granted to users who are trusted, trained, and qualified as system and network administrators

VCM is an Enterprise-wide configuration management and compliance tool. It is unsurpassed in its ability to collect, correlate and change system data on managed machines in the enterprise. VCM can configure security policies, collect and aggregate confidential information, install software and patches, and generally act as an administrative interface to an entire network of machines. This power of VCM is intended for use by trusted users that are as responsible as system and network administrators. The users must use the tool responsibly and protect their access from being subverted for unauthorized uses. In particular, VCM administrators should avoid assigning entire domain groups to VCM logins and should set the Windows login restrictions and password policies for user accounts that are VCM logins to values consistent with administrator accounts.

5.2 VCM users are advised to treat direct login prompts to VCM with skepticism and caution

When a user logs into Windows using a domain account known to VCM and then connects to VCM, the system can authorize the user by their Windows identity rather than requiring them to login explicitly to VCM. This leveraging of the Windows login system resists spoofing and cross-site scripting attacks that exploit the IE browser. VCM also accepts browser-based login when the Windows identity is either unavailable or not recognized by VCM. While this latter approach is possible, the best practice is to login (or runas) using a domain account, configure IE to transmit the login credentials, and treat browser-based login prompts with skepticism and caution.

5.3 VCM users must protect collected data as confidential information

The results of a VCM collection can contain infrastructure configuration settings, password and credential policies, encrypted password file entries, and any file uploaded from the managed machine. Even if this data is not confidential to the managed machine, it may be confidential to the machine's users. Without explicit knowledge of what is or is not sensitive, VCM users should treat and protect all collection results as confidential. Collected data should not be stored on public shares or in directories accessible to other users, including other VCM users since they may not have collection rights against the machine being the origin of the data.

5.4 Trust individual collection results no more than their source

Data collected by VCM is returned by the agent running on the managed machine. This Agent, while usually protected from tampering by non-administrative users, is ultimately subject to modification and tampering by the machine administrator or a malware infection. For this reason collected data should never be trusted more than the trust in the integrity of the source. Consider making decisions based on aggregate values rather than individual ones: how many machines have a vulnerability rather than the compliance state of a specific machine.

5.5 Beware of cross-site scripting attacks

Cross site scripting (XSS) allows an infected web site to attack a web application by injecting commands into the web application when the user temporarily browses to the infected site while still logged in to the web application. The malicious site returns hidden script and styles that invoke actions in the login session behind the user's back.

VCM users can minimize the risk of XSS attacks by taking precautions: placing the VCM web server in a trusted zone, disallowing linking into trusted zones, setting IE to transmit credentials, avoiding direct VCM login in favor of Windows logins, etc. However, even using these safeguards there is still a risk of XSS attack that warrants additional precaution. One effective step is to avoid use of the general Internet while logged in to VCM or to use VCM from within a browser or virtual machine not used for general Internet browsing. Other steps include:

- Enable IIS 'Require client certificates'
- Never placing untrusted hosts in the trusted zone
- Evaluating entering/exiting trusted zone warnings from IE
- Examining non-Windows login prompts
- Never entering VCM from external links
- Not using VCM while Internet browsing in other windows

5.6 Exported data is outside the control of VCM

VCM supports several ways to export collected data, including:

- Email notifications and alerts
- Exported or printed grids
- Exported SRS summary views and reports
- Service desk work requests
- Uploaded and exported files
- Screen snapshot

VCM users must be aware that data exported through these means are outside the scope of control of VCM.

6.0 Host Preparation and Management

VCM relies on certain host services for correct operation. This section documents the services that impact VCM's ability to operate securely, and to preserve the confidentiality, integrity, and availability of data. Hosts in different zones have different requirements, as summarized in the following table:

Host Zones and Requirements

Requirement/Zone	Infrastructure	Server	UI	Agent
Cryptographic service providers are FIPS-140 certified		X		
SQL best practices are followed (including use of firewall)		X		
Only trusted software should be installed in the server zone	X	X	X	
Perform routine backups, patches, and virus scanning	X	X	X	X

6.1 VCM hosts pass Foundation Checker checks

Before installing VCM, the VCM Foundation Checker should be run to ensure the host configuration is compatible with VCM. Do not install VCM on platforms failing the foundation checking.

6.2 Cryptographic service providers are FIPS-140 certified

All cryptographic service providers (CSPs) installed on machines in the server zone should be FIPS 140-certified. The use of FIPS cryptography is required by most government and financial organizations, and is part of the VCM Common Criteria Security Target. The Microsoft CSPs shipped with Windows 2000, 2003, XP, Vista, Windows 7, and 2008 Server meet FIPS 140-2. The assumption is that these packages have not been deleted, replaced or supplemented with non-FIPS cryptography. Since all server zone hosts are Microsoft Windows-based, you can view the list of installed crypto providers by using 'certutil -csplist'. To verify that a module is FIPS 140-certified, check the list at the National Institute of Standards and Technology Computer Security Resource Center.⁵

6.3 SQL Server best practices are followed

Direct login to the VCM SQL Server database bypasses the UI and its administrative controls. VMware recommends using a host or network firewall to prevent direct SQL Server login. In addition, customers should follow the SQL Server Security Best Practices when configuring the database instance that will store VCM data. These are available in the SQL Server 2005 SP3 Security Features and Best Practices.⁶

6.4 Only trusted software should be installed in the server zone

Even if server zone hosts are dedicated to running VCM, extra software packages beyond those provided by VMware or Microsoft are likely to be needed. Only trusted software should be installed, preferably software accompanied and verified by a software publisher certificate. It is unsafe to use software of unaccountable origin on machines in the VCM server and UI zones.

6.5 Perform routine backups, patches, and virus scanning

Routine host maintenance functions like backups, patches, and virus scanning should be performed on VCM hosts. Since UI and server zone hosts can also be managed machines, VCM itself provides the means for performing these functions.

7.0 Safeguarding Installation Kits

7.1 VCM installation kits are obtained from VMware or secure sources

Secure operation of VCM requires that the product's software be untampered with and intact as delivered by VMware. VMware ships VCM and add-on products on CD/DVD in packages signed by the VMware Software Publisher Certificate. This software reaches customer machines in various ways:

- Delivery of the CD/DVD
- Download from http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_configuration_manager/5_0
- ClickOnce™ download from the server zone
- Agent push install by the Collector service
- Patching Agent push by Patching
- Thin client UI by HTTP
- VCM Remote updates
- Patching deployed patches and updates
- VMware VCM Software Provisioning
- SMS
- Group Policy
- VCM Remote Command file attachments

The best practice is to ensure that each kit is either obtained from a secure channel, or is verified.

Executables and MSI installers can be verified by using the Certificate Verification Tool available on the Microsoft Developer's Network.⁷

The VMware Software Publisher Certificate is available at http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_configuration_manager/5_0.

7.2 VCM installation kits are protected from tampering or verified

When VCM installation kits are stored on writable media, they must be protected from tampering prior to installation. Compliance rules and other content exported using the VCM import/export tool likewise should be protected while in transit to other sites. Authenticode signatures on installation kits are verified just prior to installation. For example:

```
signtool verify /a /v "CMAgent<version>.msi"
```

7.3 Unknown software publisher warnings during ClickOnce installations are not dismissed unless the publisher is VMware

When ClickOnce software is installed through the VCM UI, IE will warn the user if the software is from an untrusted publisher (one whose Software Publisher Certificate is not in the trusted software publisher's certificate store). Despite the warning, the user can still choose to allow the software installation. However, this should not be done unless the software publisher is VMware. VMware software is identifiable as signed with the VMware Software Publisher Certificate.

7.4 Automatic upgrade of the VCM Remote Client is not used to install software

VCM Remote can push new VCM Remote Agents to the VCM Remote clients. This mechanism should not be used to distribute software other than VCM Remote.

8.0 IIS Preparation

VCM IIS web service and virtual directories should be properly prepared as described in the following sections.

8.1 IIS set to use Windows integrated authentication for the VCM Web site root

The interface to the VCM console is through a thin browser-based interface to an IIS served web application located at the /VCM virtual directory. Integrated Windows Authentication (IWA) should be used with this directory. This can be done by setting the IIS metabase property NTAuthenticationProviders to the string 'Negotiate,NTLM'. This is the default value, but VCM administrators should explicitly set this value at the /VCM directory regardless, in case subsequent modifications to the IIS metabase would unintentionally override the default value. Locate instructions for setting the metabase property in Microsoft Knowledge Base Article 215383, "How to configure IIS to support both the Kerberos protocol and the NTLM protocol for network authentication."⁸

8.2 VCM Web Service uses HTTPS

Although it is possible to use the VCM UI across HTTP, this should not be done, as collection results, configuration data, and configured passwords will travel across the network insecurely. The VCM document root should be set to require HTTPS by following the directions described in Microsoft Knowledge Base Article 324069, "How to Set Up an HTTPS Service in IIS"⁹. HTTPS not only provides security against snooping, it also assures connection to a legitimate (not spoof) instance of VCM.

In addition, an HTTPS connection activates security precautions built into IE when combined with the IE configuration recommendations listed later.

SSRS reports should also be set to use HTTPS, as described in the *VCM Hardware and Software Requirements Guide*.

8.3 SSL/HTTPS certificate issued by trusted CA or self Issued

When VCM uses SSL, TLS, or HTTPS, it authenticates machines using certificates by certificate authorities (CA). These CAs must either be internal (customer) CAs or members of the Microsoft Root Certificate Program list.¹⁰

9.0 SQL Server Preparation

9.1 Follow Microsoft SQL Server configuration best practices

Microsoft provides both guidelines and an auditing tool that ensure the secure installation and operation of SQL Server. These are available for SQL Server 2000¹¹, 2005¹², and 2008¹³.

Also, a secure installation of VCM pays particular attention to the Security Best Practices¹⁴ items regarding patching, physical security, service packs, and firewalls.

9.2 Protect SQL Server from connections originating outside the server zone

Connections to VCM's SQL Server database from outside the server zone must be prevented. Even authorized VCM users should not connect directly to the database from remote locations. A firewall is one means of accomplishing this.¹⁰ The general technique is to block TCP port 1433 and UDP port 1434.

9.3 Forbid direct SQL Server login by VCM users

Even from within the server zone, regular VCM users must not directly connect to the VCM database using tools like the Query Analyzer. Such connections bypass the administrative safeguards afforded by the VCM UI.

10.0 Web Browser Preparation

The VCM web client runs within IE and connects to the VCM web application served by IIS. Since VCM users also browse the Internet using IE, VCM requires that the security measures described in the following sections be taken in order to protect VCM users from spoofing and cross-site scripting attacks.

10.1 Place the VCM Web host in the IE trusted zone

Placing VCM in the trusted zone has beneficial effects. It allows IE to delegate the VCM user's credentials to the web service for use with SQL Server. It also allows users to disable navigation into the trusted zone from less privileged IE zones; thereby reducing XSS exposure. To place VCM web host in the IE Trusted Zone, see the *VCM Web Service Installation and Getting Started Guide*, pages 3–4, and figures 3–5. The document is available from VMware Technical Support.

10.2 Verify the VCM Web host's HTTPS certificate

The SSL certificate used for HTTPS with the VCM web host can be issued by either a trusted root certificate authority or self-issued by the customer. When a certificate from a trusted authority is detected, IE will not notify the VCM user. However, when an untrusted certificate is detected (either a customer-issued or false certificate), IE will ask the user to accept the certificate as trusted. When this occurs, VCM users should verify the certificate is authentic and authorized by clicking the 'Details' tab of the dialog and verifying the information with the certificate creator.

Trusted SSL certificates are those issued by members of the Microsoft Root Certificate Program list.

10.3 Verify the VCM software publisher certificate

Some components of the VCM UI download to the VCM user's browser as ClickOnce deployments signed by the VMware Software Publisher Certificate (SPC). When these components are activated in the UI, the user will be prompted for whether to trust the SPC. When this occurs, VCM users should verify the certificate is authentic and authorized by clicking the 'Details' tab of the dialog and verifying the information with VMware. The VMware Software Publisher Certificate is available at http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_configuration_manager/5_0.

10.4 Remove untrusted machines from the IE trusted zone

VCM is a system and network configuration management tool. Therefore, the VCM web site should be isolated from untrusted sites to prevent cross site attacks.

10.5 Customize Internet Explorer's trusted zone Internet security options

- Enable Automatic logon with current username and password
- Disable Navigate subframes across different domains
- Disable Web sites in less privileged web content zone can navigate into this zone
- Disable Display mixed content

Allowing Automatic logon enables IE to transfer credentials to machines in the trusted zone without user interaction. When this is combined with the IIS setting to use Integrated Windows Authentication, the result makes the login process resistant to spoofing and cross-site attacks. Under this configuration, login prompting does not take place within the context of the browser, but rather within the Windows login system, which is substantially resistant to such attacks. Users are advised to treat VCM login prompts with caution and skepticism since such prompts are possibly an indication of attack.

11.0 Agent Installation and Maintenance

The VCM Agent is the software installed on the managed machine to collect configuration information and securely return it to the VCM Collector. Each managed machine is its own trust zone controlled by the domain and local machine administrator. Agents do not trust other Agents, but do trust the machines in the server zone like the collector. Machines in the server zone trust the Agent to manage and return its machine's configuration data, but the Agent is not trusted as a source of data or changes to other machines, or to the VCM configuration.

The Agent is subject to its local security policies and security environment of the managed machine. The trust by the server zone in the Agent depends on the environment protecting four classes of assets:

- Agent executable code
- Machine configuration
- Collected machine data
- Agent/Collector Credentials

The Agent's executable code consists of the programs and libraries shipped in the VCM Agent installation kit. These kits and updates are signed by the VMware software publisher certificate described previously. The machine configuration is the local settings that activate the VCM Agent, grant it execution and data storage rights, and allow it to utilize infrastructure services like networking and DNS. Collected data is the settings the Agent acquires by inspecting the managed machine. Collected data is transmitted to the VCM Collector. Credentials are the certificates and private key the Agent uses to authenticate the Collector, and itself when configured for Mutual Authentication.

11.1 File and directory access controls prevent tampering

The Agent's executable code, collection results, and credentials are stored in files within the Agent installation directory. This directory and its contents must be owned by an administrative account and configured to deny read-access or modification by non-administrators.

11.2 Access control on machine configuration prevents tampering

The Agent depends on the integrity of settings in system configuration files like the Windows registry and Unix /etc directory. These settings activate the Agent and grant it access to infrastructure services like networking and DNS, as well as access to the data sources and files from which the Agent collects data. These settings must be protected from unauthorized modification.

11.3 The Agent is available for collection

The Agent operates in response to requests from the Collector service. VCM does not require the Agent to be available at all times, but it must be routinely available for collection of timely data. The environment must guarantee that the Agent is not disabled or permanently disconnected from network access or from connection requests by the Collector. The environment must also ensure the network infrastructure required for Agent-Collector communication is maintained.

11.4 The Trusted Certificate Store contains reputable certificates

The Agent validates up to two certificates while authenticating and authorizing a collector: a root certificate and an Enterprise certificate. The VCM installation allows the customer to either create a single self-signed certificate to serve as both root and Enterprise certificate, or to use a root certificate from an external public key infrastructure. In either case, the root certificate is stored in the managed machine's trusted certificate store. A certificate, whether used by VCM or not, must not be placed in that store unless it originates from an accountable certificate authority.

Presumably, a self-signed certificate is trustworthy. The reputability of other certificates can be established by verifying the issuer's membership in the Microsoft Root Certificate authority program. The current membership is listed at Windows Root Certificate Program Members <http://support.microsoft.com/kb/931125>.

Information about the admission criteria can be found at: Microsoft Root Certificate Program <http://technet.microsoft.com/en-us/library/cc751157.aspx>.

11.5 The enterprise certificate authorized collection

The Agent sends collection results only to authorized collectors. A collector is authorized if its certificate is signed by the Enterprise certificate authority. The initial Enterprise certificate is shipped with the Agent's installation kit, however, this certificate can be replaced. An administrator must install an Enterprise certificate only if they authorize every Collector certificate signed by that Enterprise certificate to access the collected data and effect change.

11.6 Unauthorized (private) Agents are not allowed

The managed machine administrator must not allow unauthorized Agents to execute, even if authentic. An Agent can be installed using an authentic Agent installation kit, but not authorized to return data (for example, a non-administrator's private Agent). As a guideline, only one Agent should be installed per managed machine, and it should be the authorized Agent.

11.7 Continuous possession and control of the Agent

The administrator must maintain possession and control of the Agent host. Even if confidentiality is preserved, loss of possession of an Agent is a threat. Continuous control of the managed machine must be maintained by physical (possession, locks) or cryptographic (encrypted file system) means.

12.0 Software Provisioning Components

The VCM Software Provisioning components consist of Package Studio, Package Manager, and software package repositories.

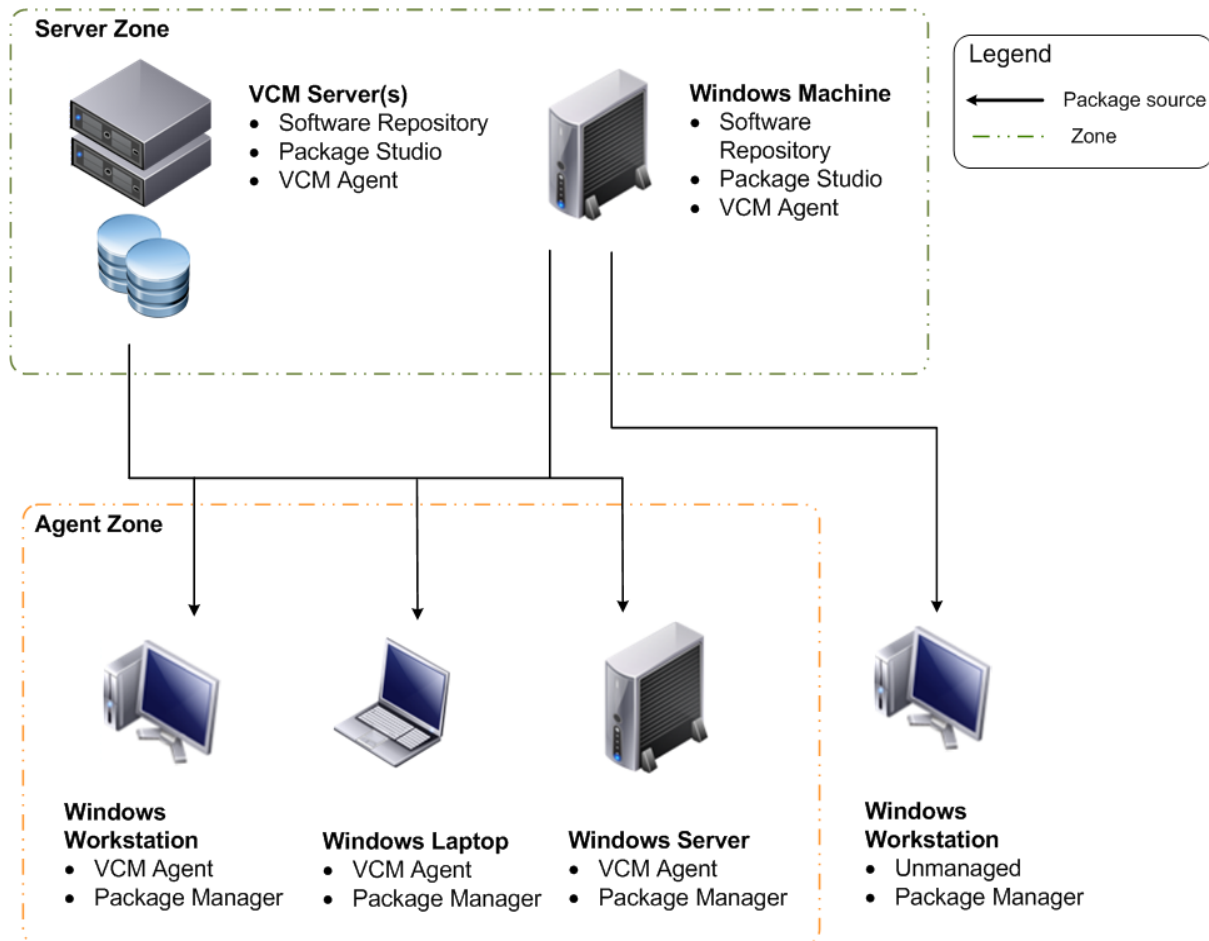


Figure 2: Software Provisioning components with respect to VCM trust zones.

A software package provides the files and scripts necessary to install and remove programs. VCM Software Provisioning components support software installed using numerous installation technologies including .msi, and .exe packages. A software repository is a shared location to which packages are published by Package Studio and the location from which Package Manager downloads packages for installation. These components can operate independent of other VCM components: repositories and target machines need not be managed by VCM agents.

Secure operation of the Software Provisioning components requires the following security environment.

12.1 All published packages are signed by trusted parties

Package Manager assumes that all packages must be signed with a private key before they are installed or uninstalled. To accommodate customers that do not use software signing or where the immediate circumstances require you to ignore that signature, override options are provided. However, secure operation of Software Provisioning requires that these practices should be followed:

- All packages should be signed
- Signatures should always be validated
- Certification authorities should be trusted

Further, repositories should not contain unsigned packages placed there independently of Package Studio.

12.2 Protect repositories

Packages in a repository are available for download by Package Manager. These repositories must be protected from tampering or unauthorized deletion of important content. Repositories should reside on access-controlled hosts protected with the measures previously described for hosts in [Hosting Environment on page 11](#).

12.3 Accept only reputable software package publishers

VMware packages are signed by the VMware Software Publisher Certificate verifiable by Verisign. This certificate is available for download from:

http://downloads.vmware.com/d/info/datacenter_downloads/vmware_vcenter_configuration_manager/5_0

Customer packages (or re-packaging of VMware Software) should be signed by the SPC's of other reputable publishers and be verifiable by Package Manager at package installation time.

12.4 Configure only trusted sources over secure channels

Package Manager is the application installed on machines to install and remove the packages stored in software repositories. Package Manager can be configured to use one or more repositories as package sources.

Only trusted repositories should be configured as sources. Further the URI specified as the package source should use a secure channel scheme like https to a repository with a trusted SSL server certificate or to a secure file share.

12.5 Take precautions when using VCM Software Provisioning Extensions

Normally VCM does not store credentials on a managed machine. However, during software provisioning actions (package management: install/remove package actions), the network authority credentials are temporarily used as local service credentials in order to authorize package installation/removal, UAC, access to network repositories, and reboot/resume activities. Service credentials are protected from disclosure to machine users, but are accessible to a determined local machine administrator using custom software.

If the managed machine or its local administrator is untrustworthy, there is a risk of loss of confidentiality of the network authority credentials during a software provisioning operation. This risk can be mitigated in several ways:

1. Do not initiate software provisioning install/remove package operations on an untrustworthy machine. Restrict provisioning operations to provisioning collections and add/remove source.
2. Assign the least permissions and login rights necessary to the network authority account used with a managed machine subject to software provisioning install/remove package operations.
3. Assign an individual network authority account using a local administrator credential to an untrustworthy machine subject to software provisioning install/remove package operations.

13.0 Operating System Provisioning Components

VCM OS provisioning deploys operating system images onto target hosts that are network booted. The target machine uses a PXE boot process to contact a DHCP server that identifies the OS Provisioning Server as the source of a bootable image, referred to as a distribution. The target machine then requests the bootable distribution across TFTP, boots the distribution, which in turn installs an operating system that is also retrieved from the OS Provisioning Server.

The OS Provisioning Server components consist of OS provisioning extensions to VCM and an OS Provisioning Server. The components are displayed in the following figure.

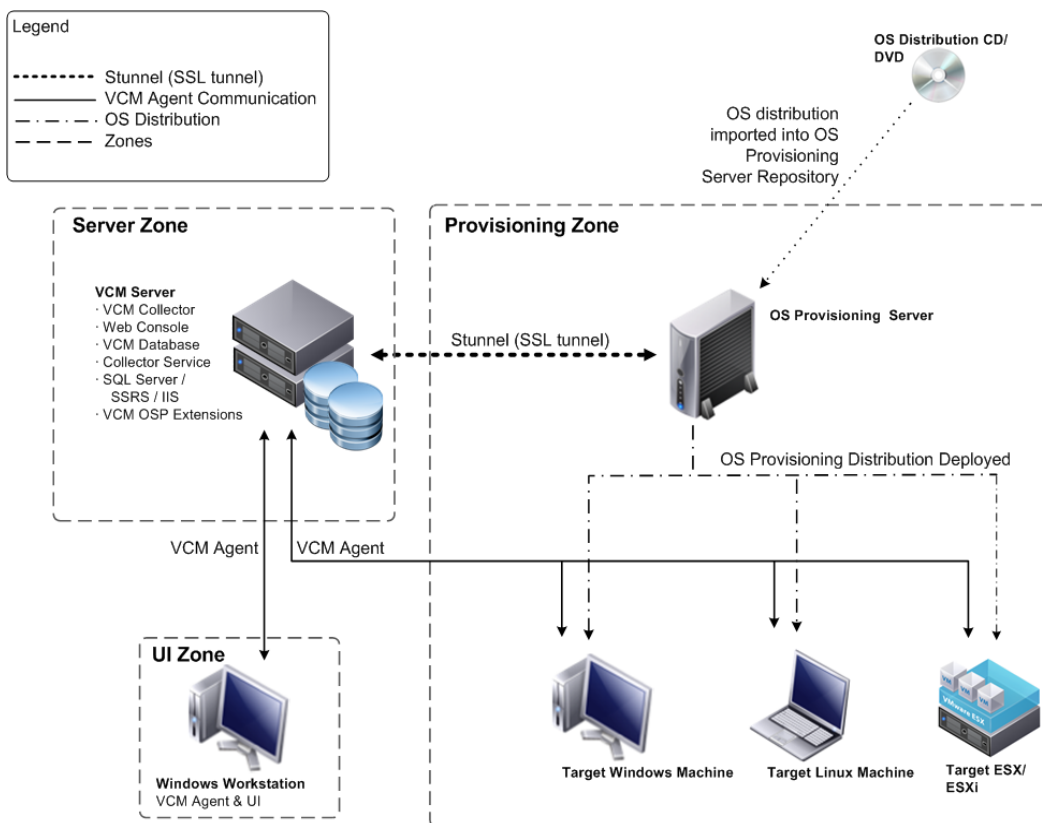


Figure 3: Operating System Provisioning Components

Secure operation of the OS provisioning components requires the following security environment.

13.1 Provisioning zone is secure

OS Provisioning operations take place across the network that connects the OS Provisioning Server and the provisionable target hosts shown in Figure 3. The provisioning zone, including its hosts, network, and network infrastructure must be protected from unauthorized access and tampering, and must be kept available and responsive. The provisioning zone network should be a private network. A separate dedicated network interface should be used to connect the OS Provisioning Server to the provisioning zone's network, as described in the *VCM Installation and Getting Started Guide* section "Private Network Interface." Access to the provisioning zone should be restricted to personnel trusted to install operating systems and act as network administrators.

13.2 Dedicated OS provisioning server host

VCM relies on the OS Provisioning Server host to protect the confidentiality, integrity, and availability of provisioning zone data and OS images. When the OS Provisioning Server host is used for purposes other than OS provisioning, you risk granting unintended access to provisioning data or images. The OS Provisioning Server host should be dedicated for provisioning operations and should not support logins except by the machine administrator and the users described in the *VCM Installation and Getting Started Guide* section "Install the OS Provisioning Server".

13.3 Close unnecessary ports on the OS provisioning server

The *VCM Installation and Getting Started Guide* declares network ports used by the OS Provisioning Server. All other ports should be kept closed using the iptables host firewall.

13.4 Protect baseline OS images

The OS Provisioning Server deploys OS images built from original distribution OS images from Microsoft, Red Hat, SUSE, VMware, and others. These images must be obtained from trusted sources over integrity protected channels and protected from tampering.

13.5 Preserve SSL tunnel

As shown in the above figure, VCM communicates with the OS Provisioning Server over an SSL tunnel using Stunnel. The "Configuring the OS Provisioning Server Integration with VCM" section in the *VCM Installation and Getting Started Guide* describes how to configure the Stunnel to listen only on address 127.0.0.1:21307 and to use SSL certificates to secure the connection. The security of this tunnel must not be defeated by weak configuration, by disabling SSL, or installing untrustworthy certificates.

13.6 Protect credentials

VCM protects and encrypts credentials stored on server zone machines. However, during OS provisioning operations, credentials within boot distributions sent to target machines are transmitted cleartext across TFTP. This is an intrinsic limitation of the PXE boot protocol and makes credentials subject to attacks that can sacrifice the confidentiality, integrity, and authenticity of the credentials or other secrets in the provisioned operating systems.

This risk must be mitigated in one of these ways:

1. Use OS provisioning only across a secure network; once a machine is provisioned, it can be transferred to an insecure network and used like any other managed machine.
2. Do not join machines to domains during provisioning operations.
3. Change secret passwords to ephemeral passwords prior to transmission by the OS Provisioning Server and change them again immediately after provisioning operations are complete.
4. Change any secret passwords transmitted during OS provisioning shortly after the process is complete. Change the passwords everywhere they were used, even on machines not involved with provisioning operations.

14.0 Proper Decommissioning

Hosts onto which VCM has been installed contain private keys, confidential credentials, and collection results. These machines must be properly decommissioned before being discarded or used for other purposes.

14.1 An installation of VCM is properly decommissioned before its hardware is repurposed or retired

VCM hosts contain confidential data and credentials from managed machines, such as:

- Collected data
- File uploads
- Private keys: Enterprise, Collector, Agent, and IIS HTTPS certificate
- Managed machine login credentials
- Proxy machine credentials
- VCM Patching patch alternate source credentials
- Secure Communication Session Cache(s)
- Network Authority Account passwords
- Collector and agent install kits
- VCM license files

Proper erasure of these values from the respective machines is a requirement for decommissioning. In this context, erasure involves more than deleting files. After transferring any sensitive data you wish to retain, best practices recommend securely erasing any disks that stored confidential data. A utility such as *sdelete1* can be used for this purpose.

14.2 Collector and Agent private keys used for TLS are not copied between machines

VCM associates a unique machine identity with private keys used with TLS. Besides being difficult to copy securely, copying a private key presents the risk of sharing it between more than one machine (a configuration that is not supported). VMware recommends you generate a distinct public/private key pair for each collector during the installation process. If TLS Mutual Authentication is being used, a distinct key pair should also be created for each Agent when the Agent kit is installed.

14.3 Enterprise certificate private key and IIS (for HTTPS) host private keys are transferred manually

If the Enterprise Certificate server is a Collector host being decommissioned, the private key must be transferred by exporting it using the MMC Certificate snap-in. This should be done using **Copy To File**, selecting .pfx file format, enabling strong protection, and selecting delete private key if export is successful. The resulting .pfx file can safely be transported to the replacement machine over a network since the file is passphrase protected.

14.4 Server zone hosts have their disks removed and transferred, secured, or erased before decommissioning

Server zone host disks contain data collected from and login credentials to managed machines. These disks should not be discarded unless they are first sanitized by a disk erasure process like SDelete¹⁵. Using these disks with a replacement Collector is a safe alternative that also preserves the previous collection results.

14.5 Erase private keys when uninstalling the Agent

When an Agent is uninstalled, its private key should be erased unless it is to be used with an updated Agent on the same host. On Windows Agents, the MCC Certificates snap-in can erase both a certificate and its private key.

14.6 Unused network authority accounts are disabled or removed

When Collectors or Agents are decommissioned, any special Network Authority accounts created specifically for the defunct machine are no longer necessary. The need for these accounts is described in the *VCM Installation and Getting Started Guide*. The accounts must be disabled or removed when no longer required. This is done from the VCM Administration panel and from the domain controllers.

References

- 1 Certificate Stores: [http://technet.microsoft.com/en-us/library/cc757138\(W.S.10\).aspx](http://technet.microsoft.com/en-us/library/cc757138(W.S.10).aspx)
- 2 Controlled Access Protection Profile: http://www.niap-ccevs.org/cc-scheme/pp/pp.cfm/id/PP_OS_CA_V1.d
- 3 Validated Products List: <http://www.niap-ccevs.org/cc-scheme/vpl/>
- 4 Products and Protection Profiles in Evaluation: http://www.niap-ccevs.org/in_evaluation/
- 5 National Institute of Standards and Technology Computer Security Resource Center: <http://csrc.nist.gov/cryptval>
- 6 SQL Server 2005 Security Best Practices: <http://download.microsoft.com/download/8/5/e/85eea4fa-b3bb-4426-97d0-7f7151b2011c/SQL2005SecBestPract.doc>
- 7 Certificate Verification Tool (Chktrust.exe): [http://msdn2.microsoft.com/en-us/library/z045761b\(vs.80\).aspx](http://msdn2.microsoft.com/en-us/library/z045761b(vs.80).aspx)
- 8 Microsoft Knowledge Base Article 215383, "How to configure IIS to support both the Kerberos protocol and the NTLM protocol for network authentication: <http://support.microsoft.com/kb/215383>
- 9 Microsoft Knowledge Base Article 324069, "How to Set up an HTTPS Server as IIS": <http://support.microsoft.com/kb/324069>
- 10 Microsoft Root Certificate Program Members: Certificate Verification Tool (Chktrust.exe) [http://msdn.microsoft.com/en-us/library/z045761b\(vs.80\).aspx](http://msdn.microsoft.com/en-us/library/z045761b(vs.80).aspx)
- 11 SQL Server 2000 Best Practices Analyzer Tool: <http://www.microsoft.com/downloads/details.aspx?familyid=b352eb1f-d3ca-44ee-893e-9e07339c1f22&displaylang=en>
- 12 SQL Server 2005 Best Practices Analyzer Tool <http://www.microsoft.com/downloads/details.aspx?FamilyId=da0531e4-e94c-4991-82fa-f0e3fbd05e63&displaylang=en>

- 13 SQL Server 2008 Best Practices Analyzer Tool:
<http://www.microsoft.com/downloads/details.aspx?FamilyID=0fd439d7-4bff-4df7-a52f-9a1be8725591&displaylang=en>
- 14 SQL Server 2005 Security Best Practices: <http://download.microsoft.com/download/8/5/e/85eea4fa-b3bb-4426-97d0-7f7151b2011c/SQL2005SecBestPract.doc>
Security Considerations for a SQL Server Installation: <http://msdn.microsoft.com/en-us/library/ms144228.aspx>
- 15 SDelete v1.51: <http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx>



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

Copyright © 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc., in the United States and/or other jurisdictions. All other marks and names mentioned herein might be trademarks of their respective companies.